



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,201	02/22/2002	Terrence A. Tomkow	RPOST-58937	3395
24201	7590	04/04/2006	EXAMINER	
FULWIDER PATTON 6060 CENTER DRIVE 10TH FLOOR LOS ANGELES, CA 90045			CHAI, LONGBIT	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 04/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	09/991,201		TOMKOW, TERRENCE A.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Longbit Chai		2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 13 February 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

### **DETAILED ACTION**

1. Original application contained claims 1 – 41. Claims 1 – 12, 15 – 23, 25 – 37 and 39 – 40 have been amended in an amendment filed on 2/13/2006. The amendment filed have been entered and made of record. Presently, pending claims are 1 – 41.

#### ***Continued Examination Under 37 CFR 1.114***

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/13/2006 has been entered.

#### ***Double Patenting***

The nonstatutory provisional double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double

Art Unit: 2131

patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1, 10, 21, 27 and 32 (and its associated dependent claims) are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 115 – 121 of copending Application No. 09/626,577 in view of Ouchi (U.S. Patent 5,978,836).

This is a provisional obviousness-type double patenting rejection. Claims of the instant application are envisioned by copending application in that claims 115 – 121 of the copending application contain all the claim limitations of the instant application except the features of (a) encrypted hash versus digital signature; however, the digital signature is deemed to be obvious in signing / encrypting the message hash using the asymmetric key (b) sending the message with either normal manner or the special manner such as taking the second path to deliver the message. However, Ouchi teaches sending the message with either normal manner or the special manner such as taking the 2<sup>nd</sup> alternative route to deliver the message selected by the user (Ouchi: Column 12 Line 3 – 15). Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those during prosecution of the copending Application.

Therefore, claims of the instant application are not patently distinct from the earlier copending application claim and as such are unpatentable for provisional obvious-type double patenting.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1 – 3 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (U.S. Patent 6618747), in view of Ouchi (U.S. Patent 5978836).

As per claim 1, Flynn teaches a method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps of:

receiving the message at the server (Flynn: Column 2 Line 20 – 23 and Figure 1 Element 20) from the sender and receiving an indication at the server from the sender that the sender wishes to send the message in a manner special to the sender and intended for the recipient and not normally provided by the server (Flynn: Column 2 Line 52 – 55: a special manner is considered as indicating a number of different recipients / attachments),

transmitting from the server to the recipient (Flynn: Figure 1 Element 30 and Column 3 Line 6 – 13: As the recipient retrieves the posted email message and attachments @ URL link, the messages are indeed delivered from the server to the recipient based on the recipient unique IP address and host name) the message in the special manner, in accordance with the indication from the sender to the server (Flynn:

Art Unit: 2131

Column 2 Line 52 – 55), an identification and address of the server (Flynn: Column 5 Line 54 – 56) and the identity of the sender (Flynn: Column 5 Line 43 and Column 2 Line 52 – 55);

sending to the sender from the server, before any authentication of the message (Flynn: Column 7 Line 16 – 18: Flynn discloses the copy of the message is forwarded to the sender from the server along with the notification of the receipt, where the message may then be compared with the message sent to verify the message was not garbled during transmission. Therefore, the message is indeed sent back to the sender from the server prior to the message authentication), a copy of the message and the information received by the server from the recipient (Flynn: Column 7 Line 14 – 15);

receiving at the server from the recipient the identity of the recipient (Flynn: Column 3 Line 33) and an indication of the receipt of the message by the recipient (Flynn: Column 3 Line 9 – 12) and the identification and address of the server (Flynn: Column 5 Line 54 – 65) and the identity of the sender. However, Flynn does not disclose expressly receiving at the server from the agent the identity of the sender.

Ouchi teaches receiving at the server from the agent the identity of the sender (Ouchi: see for example, Figure 6 Element 67 & Column 5 Line 31 – 34: sender identity must be included in the reply message).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ouchi within the system of Flynn because Ouchi teaches providing an easy accessibility of e-mail by using a flexible workflow process (Ouchi: see for example, Column 2 Line 8 – 12).

As per claim 2, Flynn teaches the transmission from the server to the agent of the recipient is in the normal manner when the sender does not provide an indication to the server that the sender wishes the server to transmit the message in the special manner to the agent of the recipient (Flynn: Column 2 Line 52 – 55: a special manner is considered as indicating a number of different recipients / attachments).

As per claim 3, Flynn does not teach the indication received by the server from the agent of the recipient includes an identification of the agent and any transferring agents through whom the message has passed between the server and the agent of the recipient.

Ouchi teaches the indication received by the server from the agent of the recipient includes an identification of the agent and any transferring agents through whom the message has passed between the server and the agent of the recipient (Ouchi: see for example, Figure 9 & Column 12 Line 11 – 15 and Column 5 Line 31 – 34).

Same rationale of combination applies herein as above in rejecting the claim 1.

As per claim 6, Flynn does not teach an additional indication is provided to the server with the message from the sender that a high priority should be provided by the server to the sending of the message by the server to the agent of the recipient and wherein the server provides the high priority in sending the message to the agent of the recipient in accordance with the additional indication.

Ouchi teaches an additional indication is provided to the server with the message from the sender that a high priority should be provided by the server to the sending of the message by the server to the agent of the recipient and wherein the server provides the high priority in sending the message to the agent of the recipient in accordance with the additional indication (Ouchi: see for example, Column 19 Line 50 – 53).

Same rationale of combination applies herein as above in rejecting the claim 1.

4. Claims 10 – 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (U.S. Patent 6618747), Ouchi (U.S. Patent 5978836), and in view of Barkan et al. (Patent Number WO 9817042).

As per claim 10, the claim limitations are met by Flynn set forth as the same reasons in the paragraph above regarding to claim 1 with the exception of the following features:

receiving at the server from the recipient a handshaking and delivery history of the transmission of the message from the server to the agent of the recipient (Flynn: Column 7 Line 14 – 15), and

transmitting from the server to the sender the message and the handshaking and delivery history of the message received by the server from the the recipient (Flynn: Column 7 Line 14 – 15; Ouchi: Column 8 Line 32 – 33 & Figure 9). However, Flynn does not teach transmitting from the server to the sender an encrypted hash of the message.



Barkan teaches transmitting from the server to the sender an encrypted hash of the message (Barkan: Page 46).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barkan within the system of Flynn as modified because (a) Flynn disclose sending a message from the server back to the sender so that this message can then be compared with the message sent to verify that the message sent was not garbled during transmission (Column 7 Line 16 – 18), and (b) Barkan teaches enhancing E-mail security for transferring registered and secure email messages mechanism using encrypted CRC by preventing the illegal copy (Barkan: see for example, Page 1 , 1<sup>st</sup> Para and Page 46 Line 1 – 2).

As per claim 11, Flynn as modified teaches the indication from the server to the server being a first indication (Ouchi: Column 12 Line 4 – 6); receiving at the server, with the message from the sender, an indication in addition to the first indication, from the server of an additional function to be performed in the transmission of the message from the server to the agent of the recipient, providing the additional function in the transmission of the message from the server to the agent of the recipient in accordance with the additional indication provided by the sender to the server (Ouchi: Column 19 Line 43 – 67).

As per claim 12, Flynn as modified teaches the message and the encrypted hash of the message are sent by the server to the sender after the server receives from the

Art Unit: 2131

recipient the handshaking and the delivery history of the transmission of the message from the server to the recipient but before the authentication of the message (Flynn: Column 7 Line 14 – 19 & Barkan: Page 46 Line 1 – 2) and wherein

the server does not retain the message or the encrypted hash after it sends the message and the encrypted hash to the sender (Barkan: Page 41 4<sup>th</sup> Para: the server is not required to store the messages in order to off-load the server);

the sender sends the message and the encrypted hash to the server for authentication of the message by the server after the server discards the messages and the encrypted hash of the message (Barkan: Page 46 & Flynn: Column 7 Line 17 – 19: Examiner notes Flynn is relied upon providing the method that the server sends the messages back to the sender and the messages may then be compared to assure the message was not garbled during the transmission and indicating other options will be apparent to those skilled in the art (Flynn: Column 7 Line 17 – 19). One obvious and well-known option in the field to validate the true message being received is by calculating the message hash / CRC and comparing with the embedded hash / CRC being sent with the message. This function could reside either at the user or at the server (to off-load the user if needed – i.e. to further forward the message from the user to the server).

5. Claims 13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (U.S. Patent 6618747), Ouchi (U.S. Patent 5978836), in view of Barkan et al. (Patent Number WO 9817042), and in view of Sasmazel et al. (U.S. Patent 6725376).

As per claim 13, Flynn does not disclose expressly the additional indication from the sender to the server provides for a recording of the transmission of the message and wherein the transmission of the message is recorded in accordance with the additional indication from the sender.

Skladman teaches the additional indication from the sender to the server provides for a recording of the transmission of the message and wherein the transmission of the message is recorded in accordance with the additional indication from the sender (Skladman: Column 11 Line 1 – 10).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Skladman within the system of Flynn as modified because Skladman teaches a more flexible unified messaging system that enable messages to be processed in accordance with the user wishes (Skladman: Abstract Line 4 – 8).

As per claim 20, Flynn as modified does not disclose expressly the server requests a delivery status notification from the agent of the recipient relating to the message when it transmits the message to the agent and wherein the server receives

Art Unit: 2131

the delivery status notification from the agent of the recipient when it receives the message from the agent.

Skladman teaches the server requests a delivery status notification from the agent of the recipient relating to the message when it transmits the message to the agent and wherein the server receives the delivery status notification from the agent of the recipient when it receives the message from the agent (Skladman: Column 11 Line 4). Same rationale of combination applies herein as above in rejecting the claim 13.

6. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (U.S. Patent 6618747), in view of Barkan et al. (Patent Number WO 9817042).

As per claim 21, Flynn teaches a method of transmitting a message through the internet to a recipient through a server displaced from the recipient, the steps at the server of:

receiving the message at the server from the sender (Flynn: Column 2 Line 20 – 23 and Figure 1 Element 20);

receiving from the sender an indication with the message from the sender that the message is to be handled by the server in a particular manner intended for the recipient and different from a normal handling of the message by the server (Flynn: Column 2 Line 52 – 55: a special manner is considered as indicating a number of different recipients / attachments), and

handling the message at the server in the particular manner intended for the recipient in accordance with the indication from the sender, to transmit the message and the digital fingerprint to the recipient (Flynn: Column 2 Line 52 – 55).

Flynn does not teach generating a hash constituting a synopsis of the message in coded form, encrypting the hash with a particular encryption code to generate an encrypted hash of the message at the server.

Barkan teaches generating a hash constituting a synopsis of the message in coded form, encrypting the hash with a particular encryption code to generate an encrypted hash of the message at the server (Barkan: Page 46).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barkan within the system of Flynn as modified because (a) Flynn disclose sending a message from the server back to the sender so that this message can then be compared with the message sent to verify that the message sent was not garbled during transmission (Column 7 Line 16 – 18), and (b) Barkan teaches enhancing E-mail security for transferring registered and secure email messages mechanism using encrypted CRC by preventing the illegal copy (Barkan: see for example, Page 1 , 1<sup>st</sup> Para and Page 46 Line 1 – 2).

As per claim 22, Flynn as modified teaches transmitting at the server the attachment and the encrypted hash of the attachment to the sender at the same time, and in the same manner, that the message and the encrypted hash of the message are

transmitted at the server to the sender (Flynn: Column 2 Line 18 – 19 & Barkan: Page 46).

7. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (U.S. Patent 6618747), in view of Barkan et al. (Patent Number WO 9817042), and in view of Ouchi (U.S. Patent 5978836).

As per claim 26, Flynn as modified teaches wherein the message is transmitted by the server in a first path to the agent of the recipient when the indication is not provided by the sender to the server with the message and wherein the message is processed by the server in a second path different from the first path when the indication is provided by the sender to the server with the message (Flynn: Column 5 Line 43 and Column 2 Line 52 – 55). However, Flynn as modified does not teach the message is processed by the server in a second path different from the first path when the indication is provided by the sender to the server with the message.

Quinch teaches the message is processed by the server in a second path different from the first path when the indication is provided by the sender to the server with the message (Ouchi: see for example, Column 12 Line 3 – 15).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ouchi within the system of Flynn as modified because Ouchi teaches providing an easy accessibility of e-mail by using a flexible workflow process (Ouchi: see for example, Column 2 Line 8 – 12).

the message, the encrypted hash of the message, the name of the sender, the identity and address of the server and the identity and internet address of the recipient are stored at the server after the passage of the message to the recipient, and the message, the encrypted hash of the message, the name of the sender, the identity and internet address of the server and the identity and address of the recipient are thereafter transmitted to the sender for storage by the sender (Flynn: Column 2 Line 20 – 23 and Figure 1 Element 20 / 30, Column 5 Line 54 – 56, Column 3 Line 33, Column 7 Line 14 – 15; Ouchi: see for example, Figure 6 Element 67 & Column 5 Line 31 – 34), and wherein

the message and the encrypted hash of the message are thereafter discarded at the server before the authentication of the message (Barkan: Page 41 4<sup>th</sup> Para and Page 46 Line 1 – 2: the server is not required to store the messages in order to off-load the server); and wherein

the message and the encrypted hash of the message are transported from the sender to the server when it is desired to authenticate the message (Barkan: Page 46 Last Para & Flynn: Column 7 Line 17 – 19: Examiner notes (a) Flynn is relied upon providing the method that the server sends the messages back to the sender and the messages may then be compared to assure the message was not garbled during the transmission and indicating other options will be apparent to those skilled in the art (Flynn: Column 7 Line 17 – 19). One obvious option in the field is to assure the actual message is by calculating the message CRC and comparing with the embedded CRC being sent with the message. This function could reside either at the user or at the

Art Unit: 2131

server (to offload the user if needed – i.e. to further forward the message from the user to the server). (b) Barken is relied upon providing the option that the server can compare and confirm the message is indeed the correct message by comparing the CRC received from the recipient (Barken: Barkan: Page 46 Last Para) which is the encrypted hash sent to the sender as part of the notification).

8. Claims 27, 32 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), in view of Ouchi (PN: 5978836), and in view of Barkan et al. (PN: WO 9817042).

As per claim 32 (and claim 27), Flynn teaches a method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:

normally transmitting to the recipient through a first path (Examiner notes the regular routine path is interpreted as the first path) from the server the message and the identity of the sender (Flynn: Column 5 Line 43 and Column 2 Line 52 – 55).

Flynn does not teach receiving at the server from the sender an indication that the message should be sent by the server to the recipient through a second path different from the first path.

Ouchi teaches receiving at the server from the sender an indication that the message should be sent by the server to the agent of the recipient through a second path different from the first path (Ouchi: see for example, Column 12 Line 10 – 15).



It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ouchi within the system of Flynn as modified because Ouchi teaches providing an easy accessibility of e-mail by using a flexible workflow process (Ouchi: see for example, Column 2 Line 8 – 12).

Accordingly, Flynn as modified teaches:

transmitting at the server to the recipient an indication of the message and the identity of the sender and the identity and address of the server through the second path different from the first path in accordance with the indication from the sender to the server.

receiving at the server (Flynn: Column 2 Line 20 – 23 and Figure 1 Element 20) from the recipient (Flynn: Figure 1 Element 30) an indication of the identity of the sender (Ouchi: see for example, Figure 6 Element 67 & Column 5 Line 31 – 34) and the identity and address of the server (Flynn: Column 5 Line 54 – 56) and the identity and address of the recipient (Flynn: Column 3 Line 33) and an indication of the status of the reception of the message at the recipient (Flynn: Column 7 Line 14 – 15).

transmitting to the sender from the server the message and the encrypted hash of the message and the information received by the server from the recipient relating to the message (Flynn: Column 7 Line 14 – 15). However, Flynn does not teach transmitting to the sender from the server the encrypted hash of the message.

Barkan teaches transmitting to the sender from the server the encrypted hash of the message (Barkan: Page 46).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barkan within the system of Flynn as modified because (a) Flynn disclose sending a message from the server back to the sender so that this message can then be compared with the message sent to verify that the message sent was not garbled during transmission (Column 7 Line 16 – 18), and (b) Barkan teaches enhancing E-mail security for transferring registered and secure email messages mechanism using encrypted CRC by preventing the illegal copy (Barkan: see for example, Page 1 , 1<sup>st</sup> Para and Page 46 Line 1 – 2).

Accordingly, Flynn a modified teaches:

providing at the server an encrypted hash of the message and the identity of the sender and the identity and the address of the server.

As per claim 33, Flynn as modified does not teach the server destroying the message and the encrypted hash of the message after the server transmits the message and the encrypted hash of the message to the sender.

Barkan teaches the server destroying the message and the encrypted hash of the message after the server transmits the message and the encrypted hash of the message to the sender but before the server authenticates the message (Barkan: Page 35, 2<sup>nd</sup> Para & Flynn: Column 7 Line 16 – 18: Flynn discloses the copy of the message is forwarded to the sender from the server along with the notification of the receipt, where the message may then be compared with the message sent to verify the message was not garbled during transmission. Therefore, the message is indeed sent

back to the sender from the server prior to the message authentication and Barkan teaches deleting all of the message related information).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barkan within the system of Flynn as modified because Barkan teaches enhancing E-mail security for transferring registered and secure email messages mechanism by preventing the illegal copy (Barkan: see for example, Page 1, 1<sup>st</sup> Para).

The sender sends the message and the encrypted hash to the server when the sender desires to have the message authenticated (Barkan: Page 46 Last Para & Flynn: Column 7 Line 17 – 19: Examiner notes (a) Flynn is relied upon providing the method that the server sends the messages back to the sender and the messages may then be compared to assure the message was not garbled during the transmission and indicating other options will be apparent to those skilled in the art (Flynn: Column 7 Line 17 – 19). One obvious option in the field is to assure the actual message is by calculating the message CRC and comparing with the embedded CRC being sent with the message. This function could reside either at the user or at the server (to offload the user if needed – i.e. to further forward the message from the user to the server). (b) Barkan is relied upon providing the option that the server can compare and confirm the message is indeed the correct message by comparing the CRC received from the recipient (Barkan: Page 46 Last Para) which is the encrypted hash sent to the sender as part of the notification).and wherein

The server authenticates the message by comparing the hashes to determine if they are identical (Sasmazel: Column 2 Line 40 – Column 3 Line 3; Barkan: Page 46).

**Examiner Notes:** This RCE amendment provides two major additional claim

limitations and both are disclosed by cited Flynn reference and therefore please refer to the previous FINAL rejection of the Office action for the claims of interests if needed.

These added two major claim limitations are: (a) sending to the sender from the server,

before any authentication of the message (Flynn: Column 7 Line 16 – 18: Flynn

discloses the copy of the message is forwarded to the sender from the server along with

the notification of the receipt, where the message may then be compared with the

message sent to verify the message was not garbled during transmission. Therefore,

the message is indeed sent back to the sender from the server prior to the message

authentication), a copy of the message and the information received by the server from

the recipient (Flynn: Column 7 Line 14 – 15) and (b) the sender sends the message and

the encrypted hash to the server for authentication of the message by the server after

the server discards the messages and the encrypted hash of the message (Flynn:

Column 7 Line 17 – 19: Examiner notes Flynn is relied upon providing the method that

the server sends the messages back to the sender and the messages may then be

compared to assure the message was not garbled during the transmission and

indicating other options will be apparent to those skilled in the art (Flynn: Column 7 Line

17 – 19). One obvious and well-known option in the field to validate the true message

being received is by calculating the message hash / CRC and comparing with the

embedded hash / CRC being sent with the message. This function could reside either

at the user or at the server (to off-load the user if needed – i.e. to further forward the

message from the user to the server).

**For reference purpose, the previous FINAL rejection is also listed as follows.**

10. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), in view of Sasmazel et al. (PN: 6725376).

As per claim 21, Flynn teaches a method of transmitting a message through the internet to a recipient through a server displaced from the recipient, the steps at the server of:

receiving the message at the server from the sender (Flynn: Column 2 Line 20 – 23 and Figure 1 Element 20);

receiving from the sender an indication with the message from the sender that the message is to be handled by the server in a particular manner different from a normal handling of the message by the server (Flynn: Column 2 Line 52 – 55: a special manner is considered as indicating a number of different recipients / attachments), and

handling the message at the server in the particular manner, in accordance with the indication from the sender, to transmit the message and the digital fingerprint to the recipient (Flynn: Column 2 Line 52 – 55).

Flynn does not teach generating a hash constituting a synopsis of the message in coded form, encrypting the hash with a particular encryption code to generate an encrypted hash of the message at the server.

Sasmazel teaches generating a hash constituting a synopsis of the message in coded form, encrypting the hash with a particular encryption code to generate an

encrypted hash of the message at the server (Sasmazel: Column 2 Line 65 – Column 3 Line 3: a more secure and efficient manner for validating the integrity of the information, as taught by Sasmazel, in using hash signature techniques).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sasmazel within the system of Flynn as modified because (a) Flynn disclose sending a message from the server back to the sender so that this message can then be compared with the message sent to verify that the message sent was not garbled during transmission (Column 7 Line 16 – 18), and (b) Sasmazel teaches transmitting data over a network and server architecture in a more secure and efficient manner for validating the integrity of the information by using hash signature techniques (Sasmazel: Column 2 Line 16 – 67).

11. Claims 4, 5, 7, 10, 11, 15 – 17, 27 – 32, 34 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), Ouchi (PN: 5978836), and in view of Sasmazel et al. (PN: 6725376).

As per claim 4, Flynn does not disclose expressly an encrypted hash of the message is provided by the server to the sender a plurality of digits in a unique sequence and is sent by the server to the sender with the message after the indication is received by the server from the agent of the recipient.

Sasmazel teaches an encrypted hash of the message is provided by the server to the sender a plurality of digits in a unique sequence and is sent by the server to the

Art Unit: 2131

sender with the message after the indication is received by the server from the agent of the recipient (Sasmazel: Column 2 Line 65 – Column 3 Line 3: a more secure and efficient manner for validating the integrity of the information, as taught by Sasmazel, in using hash signature techniques).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sasmazel within the system of Flynn as modified because (a) Flynn disclose sending a message from the server back to the sender so that this message can then be compared with the message sent to verify that the message sent was not garbled during transmission (Column 7 Line 16 – 18), and (b) Sasmazel teaches transmitting data over a network and server architecture in a more secure and efficient manner for validating the integrity of the information by using hash signature techniques (Sasmazel: Column 2 Line 16 – 67).

As per claim 5, the claim limitations are met by Flynn set forth as the same reasons in the paragraph above regarding to claim 2 with the exception of the following features: an encrypted hash of the message is provided by the server to the sender a plurality of digits in a unique sequence and is sent by the server to the sender with the message after the indication is received by the server from the agent of the recipient.

Sasmazel teaches an encrypted hash of the message is provided by the server to the sender a plurality of digits in a unique sequence and is sent by the server to the sender with the message after the indication is received by the server from the agent of the recipient (Sasmazel: Column 2 Line 65 – Column 3 Line 3: a more secure and



Art Unit: 2131

efficient manner for validating the integrity of the information, as taught by Sasmazel, in using hash signature techniques).

Same rationale of combination applies herein as above in rejecting the claim 4.

As per claim 7 and 17, Flynn as modified teaches an additional indication is provided to the server with the message from the sender that a high priority should be provided by the server to the sending of the message by the server to the agent of the recipient and wherein the server provides the high priority in sending the message to the agent of the recipient in accordance with the additional indication (Ouchi: see for example, Column 19 Line 50 – 53).

As per claim 10, the claim limitations are met by Flynn set forth as the same reasons in the paragraph above regarding to claim 1 with the exception of the following features:

receiving at the server from the agent a handshaking and delivery history of the transmission of the message from the server to the agent of the recipient (Flynn: Column 7 Line 14 – 15), and

transmitting from the server to the sender the message and the handshaking and delivery history of the message received by the server from the agent of the recipient (Flynn: Column 7 Line 14 – 15; Ouchi: Column 8 Line 32 – 33 & Figure 9). However,

Flynn does not teach transmitting from the server to the sender an encrypted hash of the message.

Sasmazel teaches transmitting from the server to the sender an encrypted hash of the message (Sasmazel: Column 2 Line 65 – Column 3 Line 3: a more secure and efficient manner for validating the integrity of the information, as taught by Sasmazel, in using hash signature techniques).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sasmazel within the system of Flynn because (a) Flynn disclose sending a message from the server back to the sender so that this message can then be compared with the message sent to verify that the message sent was not garbled during transmission (Column 7 Line 16 – 18), and (b) Sasmazel teaches transmitting data over a network and server architecture in a more secure and efficient manner for validating the integrity of the information by using hash signature techniques (Sasmazel: Column 2 Line 16 – 67).

As per claim 11 and 16, Flynn as modified teaches the indication from the server to the server being a first indication (Ouchi: Column 12 Line 4 – 6); receiving at the server, with the message from the sender, an indication in addition to the first indication, from the server of an additional function to be performed in the transmission of the message from the server to the agent of the recipient, providing the additional function in the transmission of the message from the server to the agent of the recipient in

accordance with the additional indication provided by the sender to the server (Ouchi: Column 19 Line 43 – 67).

As per claim 15, Flynn as modified teaches the additional indication from the sender provides for the message to be sent by the server to the agent for the recipient by a special route and wherein the message is sent by the special route from the server to the agent of the recipient in accordance with the additional indication from the sender (Flynn: Column 5 Line 43 and Column 2 Line 52 – 55; Ouchi: see for example, Column 12 Line 3 – 15).

As per claim 32 (and claim 27), Flynn teaches a method of transmitting a message from a sender to an agent for a recipient through a server displaced from the agent, including the steps at the server of:

normally transmitting to the agent of the recipient through a first path (Examiner notes the regular routine path is interpreted as the first path) from the server the message and the identity of the sender (Flynn: Column 5 Line 43 and Column 2 Line 52 – 55).

Flynn does not teach receiving at the server from the sender an indication that the message should be sent by the server to the agent of the recipient through a second path different from the first path.

Ouchi teaches receiving at the server from the sender an indication that the message should be sent by the server to the agent of the recipient through a second path different from the first path (Ouchi: see for example, Column 12 Line 10 – 15).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ouchi within the system of Flynn as modified because Ouchi teaches providing an easy accessibility of e-mail by using a flexible workflow process (Ouchi: see for example, Column 2 Line 8 – 12).

Accordingly, Flynn as modified teaches:

transmitting at the server to the agent of the recipient an indication of the message and the identity of the sender and the identity and address of the server through the second path different from the first path in accordance with the indication from the sender to the server.

receiving at the server (Flynn: Column 2 Line 20 – 23 and Figure 1 Element 20) from the agent of the recipient (Flynn: Figure 1 Element 30: an recipient agent is considered as the software entity associated with the recipient machine) an indication of the identity of the sender (Ouchi: see for example, Figure 6 Element 67 & Column 5 Line 31 – 34) and the identity and address of the server (Flynn: Column 5 Line 54 – 56) and the identity and address of the agent (Flynn: Column 3 Line 33) and an indication of the status of the reception of the message at the agent (Flynn: Column 7 Line 14 – 15).

transmitting to the sender from the server the message and the encrypted hash of the message and the information received by the server from the agent of the

recipient relating to the message (Flynn: Column 7 Line 14 – 15). However, Flynn does not teach transmitting to the sender from the server the encrypted hash of the message.

Sasmazel teaches transmitting to the sender from the server the encrypted hash of the message (Sasmazel: Column 2 Line 65 – Column 3 Line 3: a more secure and efficient manner for validating the integrity of the information, as taught by Sasmazel, in using hash signature techniques).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sasmazel within the system of Flynn because (a) Flynn disclose sending a message from the server back to the sender so that this message can then be compared with the message sent to verify that the message sent was not garbled during transmission (Column 7 Line 16 – 18), and (b) Sasmazel teaches transmitting data over a network and server architecture in a more secure and efficient manner for validating the integrity of the information by using hash signature techniques (Sasmazel: Column 2 Line 16 – 67).

Accordingly, Flynn a modified teaches:

providing at the server an encrypted hash of the message and the identity of the sender and the identity and the address of the server.

As per claim 28, Flynn as modified teaches the encrypted hash of the message includes a hash of the message and an encryption of the hash (Barkan: see for example, Page 46 1<sup>st</sup> Para) and wherein the message and the encrypted hash of the message and the identity of the sender and the identity and address of the server

and the identity and the address of the agent of the recipient and the and Page 51  
1<sup>st</sup> Para at the agent of the reception at the agent of the message are transmitted by  
the server to the sender (Sasmazel: Column 2 Line 65 – Column 3 Line 3, Flynn:  
Column 2 Line 20 – 23 and Figure 1 Element 20 / 30, Column 5 Line 54 – 56,  
Column 3 Line 33, Column 7 Line 14 – 15; Ouchi: see for example, Figure 6 Element  
67 & Column 5 Line 31 – 34).

As per claim 29 – 31, the claim limitations are met as the same reasons as that  
set forth in rejecting claim 27 and 28.

As per claim 34, Flynn as modified teaches the server receives additional  
information from the sender relating to additional functions to be performed by the  
server on the message in the transmission of the message from the server to the agent  
of the recipient and wherein the server performs the additional functions on the  
message, in accordance with the additional information received by the server from the  
sender, in the transmission of the message from the server to the agent of the recipient  
(Flynn: Column 5 Line 43 and Column 2 Line 52 – 55; Ouchi: see for example, Column  
12 Line 3 – 15 and Column 19 Line 43 – 67).

As per claim 35, Flynn as modified teaches the indication received by the server  
from the sender constitutes a first coding of the message from the sender and wherein  
the additional information received by the server from the sender of the additional  
function to be performed by the server constitutes a second coding, added to the first

Art Unit: 2131

coding, of the message from the sender (Flynn: Column 5 Line 43 and Column 2 Line 52 – 55; Ouchi: see for example, Column 12 Line 3 – 15 and Column 19 Line 43 – 67).

12. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), Ouchi (PN: 5978836), in view of Skladman et al. (PN: 6438215).

As per claim 8 and 9, Flynn does not disclose expressly an additional indication is provided to the server with the message from the sender that the sending of the message by the server to the agent of the recipient should be recorded by the server and wherein the server records the sending of the message to the agent of the recipient in accordance with the additional indication.

Skladman teaches an additional indication is provided to the server with the message from the sender that the sending of the message by the server to the agent of the recipient should be recorded by the server and wherein the server records the sending of the message to the agent of the recipient in accordance with the additional indication (Skladman: Column 11 Line 1 – 4).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Skladman within the system of Flynn as modified because Skladman teaches a more flexible unified messaging system that enable messages to be processed in accordance with the user wishes (Skladman: Abstract Line 4 – 8).

13. Claims 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), in view of Sasmazel et al. (PN: 6725376), and in view of Olkin et al. (PN: 6584564).

As per claim 22, Flynn as modified teaches generating at the server for any message an encrypted hash. However, Flynn as modified does not disclose expressly generating at the server for any attachment to the message, an encrypted hash of the attachment.

Olkin teaches generating at the server for any attachment to the message, an encrypted hash of the attachment (Olkin: see for example, Column 14 Line 50 – 60).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Olkin within the system of Flynn as modified because Olkin teaches providing a flexible and secure protection scheme for a wide range of E-mail applications (Olkin: see for example, Column 3 Line 36 – 38).

Accordingly, Flynn as modified teaches:

transmitting at the server the attachment and the encrypted hash of the attachment to the sender at the same time, and in the same manner, that the message and the encrypted hash of the message are transmitted at the server to the sender (Flynn: Column 5 Line 54 – 56 and Column 7 Line 15 – 16; Olkin: Column 3 Line 36 – 38).



As per claim 23, Flynn as modified teaches the message is handled by the server in the normal manner when the indication is not provided by the sender to the server with the message and wherein the message is handled by the server in the particular manner when the indication is provided by the sender to the server with the message (Flynn: Column 2 Line 52 – 67).

14. Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), in view of Sasmazel et al. (PN: 6725376), and in view of Ouchi (PN: 5978836).

As per claim 25, Flynn as modified teaches storing at the server the encrypted hash of the message, the name of the sender, the identity and address of the server and the identity and internet address of the recipient, and transmitting to the sender for storage by the sender the message, the encrypted hash of the message, the name of the sender, the identity and address of the server and the identity and internet address of the recipient (Sasmazel: Column 2 Line 65 – Column 3 Line 3, Flynn: Column 2 Line 20 – 23 and Figure 1 Element 20 / 30, Column 5 Line 54 – 56, Column 3 Line 33, Column 7 Line 14 – 15). However, Flynn does not disclose expressly receiving at the server from the agent the name of the sender.

Ouchi teaches receiving at the server from the agent the name of the sender (Ouchi: see for example, Figure 6 Element 67 & Column 5 Line 31 – 34: sender identity must be included in the reply message).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ouchi within the system of Flynn as modified because Ouchi teaches providing an easy accessibility of e-mail by using a flexible workflow process (Ouchi: see for example, Column 2 Line 8 – 12).

As per claim 26, Flynn as modified teaches wherein the message is transmitted by the server in a first path to the agent of the recipient when the indication is not provided by the sender to the server with the message and wherein the message is processed by the server in a second path different from the first path when the indication is provided by the sender to the server with the message (Flynn: Column 5 Line 43 and Column 2 Line 52 – 55). However, Flynn as modified does not teach the message is processed by the server in a second path different from the first path when the indication is provided by the sender to the server with the message.

Quinch teaches the message is processed by the server in a second path different from the first path when the indication is provided by the sender to the server with the message (Ouchi: see for example, Column 12 Line 3 – 15).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ouchi within the system of Flynn as modified because Ouchi teaches providing an easy accessibility of e-mail by using a flexible workflow process (Ouchi: see for example, Column 2 Line 8 – 12).

the encrypted hash of the message, the name of the sender, the identity and address of the server and the identity and internet address of the recipient are stored at

the server, and the message, the encrypted hash of the message, the name of the sender, the identity and internet address of the server and the identity and address of the recipient are transmitted to the sender for storage by the sender (Sasmazel: Column 2 Line 65 – Column 3 Line 3, Flynn: Column 2 Line 20 – 23 and Figure 1 Element 20 / 30, Column 5 Line 54 – 56, Column 3 Line 33, Column 7 Line 14 – 15; Ouchi: see for example, Figure 6 Element 67 & Column 5 Line 31 – 34).

15. Claims 12, 13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), Ouchi (PN: 5978836), in view of Sasmazel et al. (PN: 6725376), and in view of Skladman et al. (PN: 6438215).

As per claim 12, Flynn does not disclose expressly the server does not retain the message after it sends the message to the sender; the message is sent by the server to the sender after the server receives from the agent of the recipient the handshaking and the delivery history of the transmission of the message from the server to the agent of the recipient.

Skladman teaches the server does not retain the message after it sends the message to the sender; the message is sent by the server to the sender after the server receives from the agent of the recipient the handshaking and the delivery history of the transmission of the message from the server to the agent of the recipient (Skladman: Column 11 Line 1 – 10).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Skladman within the system of Flynn as modified because Skladman teaches a more flexible unified messaging system that enable messages to be processed in accordance with the user wishes (Skladman: Abstract Line 4 – 8).

As per claim 13, Flynn does not disclose expressly the additional indication from the sender to the server provides for a recording of the transmission of the message and wherein the transmission of the message is recorded in accordance with the additional indication from the sender.

Skladman teaches the additional indication from the sender to the server provides for a recording of the transmission of the message and wherein the transmission of the message is recorded in accordance with the additional indication from the sender (Skladman: Column 11 Line 1 – 10).

Same rationale of combination applies herein as above in rejecting the claim 12.

As per claim 20, Flynn as modified does not disclose expressly the server requests a delivery status notification from the agent of the recipient relating to the message when it transmits the message to the agent and wherein the server receives the delivery status notification from the agent of the recipient when it receives the message from the agent.

Skladman teaches the server requests a delivery status notification from the agent of the recipient relating to the message when it transmits the message to the agent and wherein the server receives the delivery status notification from the agent of the recipient when it receives the message from the agent (Skladman: Column 11 Line 4).

Same rationale of combination applies herein as above in rejecting the claim 12.

16. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), Ouchi (PN: 5978836), in view of Sasmazel et al. (PN: 6725376), and in view of Merriam (PN: 6609138).

As per claim 14, Flynn does not teach the additional indication from the sender provides for an archiving of the message and wherein the message is archived in accordance with the additional indication from the sender.

Merriam teaches the additional indication from the sender provides for an archiving of the message and wherein the message is archived in accordance with the additional indication from the sender (Merriam: see for example, Abstract Line 15 – 18).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Merriam within the system of Ouchi because Merriam teaches providing an automated manager for an E-mail archive repository (Merriam: see for example, Column 2 Line 37 – 39).

Art Unit: 2131

17. Claims 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), Ouchi (PN: 5978836), in view of Sasmazel et al. (PN: 6725376), and in view of Barkan et al. (PN: WO 9817042).

As per claim 18 and 19, Flynn does not teach destroying the message and the encrypted hash of the message and the handshaking and delivery history of the message.

Barkan teaches destroying the message and the encrypted hash of the message and the handshaking and delivery history of the message (Barkan: Page 35, 2<sup>nd</sup> Para: Barkan teaches deleting all of the message related information).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barkan within the system of Flynn as modified because Barkan teaches enhancing E-mail security for transferring registered and secure email messages mechanism by preventing the illegal copy (Barkan: see for example, Page 1 , 1<sup>st</sup> Para).

18. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), in view of Sasmazel et al. (PN: 6725376), in view of Olkin et al. (PN: 6584564), and in view of Ouchi (PN: 5978836).

As per claim 24, Flynn as modified teaches the message is processed by the server in a first path when the indication is not provided by the sender to the server with the message and wherein (Flynn: Column 5 Line 43 and Column 2 Line 52 – 55).

Flynn does not teach receiving at the server from the sender an indication that the message should be sent by the server to the agent of the recipient through a second path different from the first path.

Ouchi teaches receiving at the server from the sender an indication that the message should be sent by the server to the agent of the recipient through a second path different from the first path (Ouchi: see for example, Column 12 Line 10 – 15).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ouchi within the system of Flynn as modified because Ouchi teaches providing an easy accessibility of e-mail by using a flexible workflow process (Ouchi: see for example, Column 2 Line 8 – 12).

19. Claims 33 and 36 – 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), in view of Ouchi (PN: 5978836), in view of Sasmazel et al. (PN: 6725376), and in view of Barkan et al. (PN: WO 9817042).

As per claim 33, Flynn as modified does not teach the server destroying the message and the encrypted hash of the message after the server transmits the message and the encrypted hash of the message to the sender.

Barkan teaches the server destroying the message and the encrypted hash of the message after the server transmits the message and the encrypted hash of the message to the sender (Barkan: Page 35, 2<sup>nd</sup> Para: Barkan teaches deleting all of the message related information).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barkan within the system of Flynn as modified because Barkan teaches enhancing E-mail security for transferring registered and secure email messages mechanism by preventing the illegal copy (Barkan: see for example, Page 1, 1<sup>st</sup> Para).

The server authenticates the message by comparing the hashes to determine if they are identical (Sasmazel: Column 2 Line 40 – Column 3 Line 3; Barkan: Page 46).

As per claim 36, the claim limitations are met as the same reasons as that set forth in rejecting claim 34 and 35.

As per claim 37, Flynn as modified does not teach the sender transmits the encrypted hash of the message to the server when the sender wishes to have the message authenticated wherein the server operates upon the message and encrypted hash of the message to have the message authenticated.

Barkan teaches the sender transmits the encrypted hash of the message to the server when the sender wishes to have the message authenticated wherein the server operates upon the message and encrypted hash of the message to have the message



authenticated (Barkan: Page 45 and 46; Sasmazel: Column 2 Line 40 – Column 3 Line 3;).

Same rationale of combination applies herein as above in rejecting the claim 33.

As per claim 38, Flynn as modified teaches the server provides a first hash of the message and decrypts the encrypted hash to provide a second hash of the of the message and compares the first and second hashes to authenticate the message (Barkan: Page 45 and 46; Sasmazel: Column 2 Line 40 – Column 3 Line 3);

20. Claims 39 – 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flynn et al. (PN: 6618747), in view of Sasmazel et al. (PN: 6725376), in view of Ouchi (PN: 5978836), and in view of Barkan et al. (PN: WO 9817042).

As per claim 39, Flynn as modified does not teach the message and the encrypted hash of the message are destroyed by the server after the message and the encrypted hash of the message are transmitted to the sender.

Barkan teaches the message and the encrypted hash of the message are destroyed by the server after the message and the encrypted hash of the message are transmitted to the sender (Sasmazel: Column 2 Line 40 – Column 3 Line 3; Barkan: Page 35, 2<sup>nd</sup> Para: Barkan teaches deleting all of the message related information).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Barkan within the system of Flynn as

Art Unit: 2131

modified because Barkan teaches enhancing E-mail security for transferring registered and secure email messages mechanism by preventing the illegal copy (Barkan: see for example, Page 1, 1<sup>st</sup> Para).

As per claim 40 and 41, the claim limitations are met as the same reasons as that set forth in rejecting claim 37 and 38.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.




If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai  
Examiner  
Art Unit 2131

LBC

  
  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100